LISTING OF PENDING CLAIMS

The following is a listing of the currently pending claims in this application:

1. (Currently Amended) A communications network security method for ascertaining the integrity of a first communications network and identifying potential security risks across a perimeter of the first communications network, the method comprising:

identifying a plurality of routes that define ~~a~~ the first communications network;

identifying a plurality of hosts associated with the first communications network as a function of the plurality of routes;

receiving a census of the first communications network as a function of the plurality of hosts to determine a topology of the first communications network;

probing at least one first host of the plurality hosts of the first communications network by transmitting a packet to the first host, the first host being selected from the census results and the packet having at least a source address of a second host which is associated with a second communications network, wherein the source address is selected independent of any request from the second host to the first host; and

determining a security characteristic of the probed first host as a function of a response by the probed first host in receiving the packet, the security characteristic being a measure of connectivity between the first communications network and the second communications network, the measure of connectivity being an indication of connectivity between the first communications network and the second communications network.

2. (Currently Amended) The method of claim 1 wherein the source address of the second host is ~~an~~ a return IP address ~~associated with a host~~ external to the first communications network~~, and the external host being associated with the second communications network~~.

3. (Currently Amended) The method of claim 2 wherein the response of the probed first host to the receipt of the packet includes transmitting a second packet, the

second packet being derived using at least a portion of information from the received packet.

4. (Cancelled).

5. (Cancelled).

6. (Currently Amended) The method of claim ~~5~~ 2 wherein the measure of connectivity is determined by the further operation of:

monitoring the probed first host to determine the response, and if the response includes a transmission of a second packet from the probed first host to the second host at the return IP address, generating a security alert message identifying the probed first host as a security risk.

7. (Previously Presented) The method of claim 3 wherein the first communications network and the second communications network have different security levels.

8. (Previously Presented) The method of claim 3 wherein the transmitted packet is a TCP packet which returns a TCP packet in response thereto.

9. (Previously Presented) The method of claim 3 wherein the second packet is a UDP packet or an ICMP packet, which returns either a UDP packet or ICMP packet in response thereto.

10. (Currently Amended) A method for analyzing network security across a perimeter of a first communications network utilizing a security host, the method comprising:

receiving a census of the first communications network;

transmitting, from the security host, a packet ~~from~~ associated with a host of a second communications network to a particular one host of a plurality of hosts internal to

the first communications network, the internal host being selected from the census, and the packet ~~being generated as a function of both~~ having an IP source address associated with the host of the second communications network, wherein ~~and an IP address associated with the internal host of the first communications network~~the IP source address is selected independent of any request from the host of the second communications network to the internal host of the first communications network; and

determining a security characteristic of the particular one internal host of the first communications network as a function of a response by the internal host to the receipt of the packet, the security characteristic being a measure of connectivity between the first communications network and the second communications network, the measure of connectivity being an indication of connectivity between the first communications network and the second communications network.

11. (Currently Amended) The method of claim 10 wherein the measure of connectivity is a function of whether the internal host of the first communications network communicates with the host of the second communications network, and the measure of connectivity being determined by the further operation of:

monitoring the internal host to determine the response, and if the response includes a transmission of a second packet, utilizing the IP source address, from the internal host to the host of the second communications network, generating a security alert message identifying the internal host as a security risk.

12. (Original) The method of claim 11 wherein the second packet is derived using at least a portion of information from the transmitted packet.

13. (Cancelled).

14. (Previously Amended) The method of claim 12 wherein the internal host is a dual-homed host.

15. (Previously Presented) The method of claim 11 wherein the security characteristic includes an indication that the internal host is outside any security measures provided by a firewall associated with the first communications network.

16. (Currently Amended) A communications system for ascertaining the integrity of a first communications network and identifying potential security risks across a perimeter of the first communications network, the communications system comprising:

a first plurality of computers associated with ~~a~~ the first communications network;

a second plurality of computers associated with a second communications network; and

a security host computer which determines a security characteristic of a first computer from the first plurality of computers, the security characteristic being a measure of connectivity between the first communications network and the second communications network by probing the first computer by transmitting a packet to the first computer, the first computer being selected from a census of the first communications network and the packet being generated as a function of both an IP source address associated with a second computer of the second plurality of computers, wherein said IP source address is selected independent of any request from the second computer to the first computer, and an IP address associated with the first computer, and determining the measure of connectivity as a function of a response of the first computer to receiving the packet, the measure of connectivity being an indication of connectivity between the first communications network and the second communications network.

17. (Original) The communications system of claim 16 wherein the security host computer is associated with the first communications network.

18. (Previously Presented) The communications system of claim 17 wherein the response of the first computer to the receipt of the packet includes transmitting a second packet, the second packet being derived using at least a portion of information from the received packet.

19. (Previously Presented) The communications system of claim 18 wherein the security host computer determines the measure of connectivity by monitoring the probed first computer to determine the response, and if the response includes the transmission of the second packet from the probed host, generating a security alert message identifying the first computer as a security risk.

20. (Previously Presented) The communications system of claim 17 wherein the first communications network is an intranet and the second communications network is an Internet, and the first communications network and the second communications network have different security levels.

21. (Currently Amended) A security host computer for ascertaining the integrity of a first communications network and identifying potential security risks across a perimeter of the first communications network, the security host computer comprising:

means for performing a census of ~~a~~ the first communications network and determining a topology of the first communications network, the topology being defined by at least one computer,

means for probing the at least one computer by transmitting a packet to the computer, the computer being selected from the census results and the packet being generated as a function of (i) the topology, (ii) an IP source address associated with a particular host computer associated with a second communications network, wherein the IP source address is selected independent of any request from the second computer to the first computer, and (iii) an IP address associated with the computer, the second communications network being separate from the first communications network; and

a monitor for determining a security level of the computer as a function of a response by the computer to the receipt of the packet, and the security level being a measure of connectivity between the first communications network and the second communications network, the measure of connectivity being an indication of connectivity between the first communications network and the second communications network.

22. (Currently Amended) The security host computer of claim 21 wherein the measure of connectivity is determined by monitoring the computer's response, and if the response includes a transmission of a second packet, utilizing the IP source address, from the computer, a security alert message identifying the computer as a security risk is generated.

23. (Previously Presented) The security host computer of claim 22 wherein the first communications network and the second communications network have different security levels.

24. (Currently Amended) A machine-readable medium having stored thereon a plurality of instructions, the plurality of instructions including instructions that, when executed by a machine, cause the machine to perform of a method for analyzing a first communications network's integrity and identifying potential security risks across a perimeter of the first communications network by receiving a census of the first communications network; probing a first host of the first communications network by transmitting a packet to the first host, the host being selected from the census results and the packet being derived as a function of a topology of the first communications network and the packet having a source address which is associated with a second host of a second communications network, wherein the source address is selected independent of any request from the second host to the first host; and determining the first communications network's integrity as a function of a response by the probed host in receiving the packet wherein the response indicates a measure of connectivity between the first communications network communicates and the second communications network, and the measure of connectivity being an indication of connectivity between the first communications network and the second communications network.

25. (Cancelled) .

26. (Currently Amended) The machine-readable medium of claim 24 wherein the response of the probed first host to the receipt of the packet includes transmitting a

second packet, the second packet being derived using at least a portion of information from the received packet.

27. (Previously Presented) The machine-readable medium of claim 26 wherein the first communications network is an intranet, and the second communications network is an Internet.